

530 Virginia Road, P.O. Box 9133
Concord, MA 01742-9133

FEB 13 2006

Telephone: (978) 341-0036

Facsimile: (978) 341-0136

UNOFFICIAL DOCUMENT FOR EXAMINER'S REVIEW**FACSIMILE COVER SHEET****Examiner:** Ronald Baum **Group:** 2136**Date:** February 13, 2006**Client Code:** 3602**Facsimile No.:** (571) 273-8300**From:** David J. Thibodeau, Jr.
Reg. No. 31,671**Subject:** Docket No.: 3602.1002-000
Applicants: Nicholas Stamos, et al.
Serial No.: 10/750,321
Filing Date: December 31, 2003Number of pages including this cover sheet: 5Please confirm receipt of facsimile: Yes X No _____**Comments:**

Dear Examiner Baum,

Thank you for our discussion on Thursday, February 9, 2006. As I mentioned, we are planning to file a Request for Continued Examination, and enclosed herewith is a set of claims that we propose to submit. I would appreciate the opportunity to speak with you once again as to whether the amended claims would now better distinguish the Teal U.S. Patent Publication 2003/0120935 prior art. I will call you later this week to arrange a convenient time for that call.

Thank you for your assistance in this matter.



David J. Thibodeau, Jr., Esq.

Reg. No. 31,671

Privileged and Confidential - All information transmitted hereby is intended only for the use of the addressee(s) named above. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient(s), please note that any distribution or copying of this communication is strictly prohibited. Anyone who received this communication in error is asked to notify us immediately by telephone and to destroy the original message or return it to us at the above address via first class mail.

(Original claims 1-12 to be cancelled)

(Proposed new claims to be filed with Request for Continued Examination)

Formatted: w-w-Body Text First
Indent: Indent. Left: 0"

13. A process for controlling access to digital assets in a network of data processing devices, the process comprising:

defining a security perimeter that includes two or more data processing devices;

defining one or more digital asset encryption policies, to be applied to digital assets when a possible risk in use of a digital asset by an end user occurs;

sensing atomic level digital asset access events, the sensing step located within an operating system kernel in an end user client device, at a point of authorized access to the digital asset by the end user;

aggregating multiple atomic level events to determine a sequence of digital asset access events;

if the sequence of digital asset access events matches a predefined digital asset usage policy that indicates a risk of use of the digital asset outside of the security perimeter;

asserting one of the digital asset encryption policies associated with the sequence of events, by encrypting the digital asset, prior to allowing access to the digital asset from outside the security perimeter.

Deleted: n

Deleted: user

Deleted: assets

Deleted: data processing environment

Deleted: 1

Deleted: asset

Deleted: w.u

Formatted: Font: Not Bold

Deleted: c

Deleted: combined events

Deleted: and

Deleted:

Deleted: an

Deleted: policy if at least one combined event has occurred that matches a predefined digital asset usage risk policy

Formatted: Indent. Left: 0.5"

14. A method as in claim 13 wherein the digital assets are application level data files to which the user has read and write access within the security perimeter

15. A method as in claim 13 additionally comprising the steps of:
storing the digital asset encryption policies in a policy server device in the network, and
within the operating system kernel of the end user client device.

receiving the stored digital asset encryption policies from the policy server over a secure network connection.

16. A process as in Claim 13 wherein the step of asserting the digital asset encryption policy, by encrypting the digital asset prior to providing access, is implemented in an operating system kernel of the client user device.

17. A method as in claim 13 wherein
the sequence of digital access events indicates that the end user is attempting to
store a copy of the digital asset, and
the digital asset encryption policy specifies whether the digital asset is to be
encrypted or not, depending upon a type of storage device on which the end user is
attempting to store a copy.

18. A method as in claim 17 wherein the encryption policy specifies that the digital asset is not to be encrypted when the type of storage device is a local file server.

19. A method as in claim 17 wherein the encryption policy specifies that the digital asset is to be encrypted when the type of storage device is a removable media storage device.

20. A method as in claim 13 wherein
the sequence of access events indicates that the end user is sending the digital asset through a network communication port, and
the encryption policy further specifies that the digital asset is to be encrypted prior to sending the digital asset through the network communication point.

21. A method as in claim 20 wherein
the sequence of access events indicates that the end user is attaching the digital asset to one of an electronic mail message or instant messaging service.

Deleted: 1

Deleted: 2

Deleted: 1

22. A method as in claim 13 wherein
the sequence of access events includes a first file open event, followed by a
clipboard copy operation, a second file open event, and a file transmit through network
communication event.

23. A method as in claim 13 wherein
one of the encryption policies specifies that encryption is to be applied to an
asset when a particular sequence of access events is sensed; and
another of the encryption policies specifies that encryption is not to be applied to
an asset when another particular sequence of access events is sensed.

24. A process as in Claim 13 that operates independently of application software.

25. A process as in Claim 13 additionally comprising:
determining a sensitivity level of a particular digital asset in the step of
sensing atomic level digital asset access events; and
asserting one of the digital asset encryption policies by either encrypting
the digital asset or not, depending upon the sensitivity of the particular digital
asset.

26. A process as in Claim 13, additionally comprising:
forwarding the digital asset to a second client end user device, and

Deleted: 5 A process as in Claim 1
additionally comprising 1
encrypting an associated digital asset 1
1
1
4. A process as in Claim 1 wherein the
combined event is a time sequence of
multiple atomic level events 1
Formatted: Indent: First line: 0"
Deleted: 5
Deleted: 2
Deleted: 1
0 A process as in Claim 1 wherein the
sensing, aggregating, and asserting steps
operate in real time. 1
Deleted: 7
Deleted: 1
Deleted: adaptive encryption
Deleted: to
Deleted: optionally
Deleted: 1
8 A process as in Claim 1 wherein the
combined event specifies an action to be
taken with the digital asset 1
Deleted: 9 A process as in Claim 2
additionally comprising 1
at the client user device, applying
encryption of the encryption policy
specified the digital asset to be encrypted 1
Deleted: 10
Deleted: 9

asserting an encryption policy at the second client ~~end user~~ device.

27 A process as in Claim 26 additionally comprising:
applying decryption at the second client user device.

28. A process as in Claim 13 additionally comprising:
forwarding the digital asset to a second client user device; and
not asserting an encryption policy at the second client user device, so
that if the encryption policy specifies encryption, the digital asset cannot be read
at the second client user device.

Deleted: 1
Formatted: Indent, Left: 0"
Formatted: Bullets and Numbering
Deleted: 10
Formatted: Indent, Left: 0"
Deleted: 1
Formatted: Bullets and Numbering
Deleted: 9